SECS1028 - Laboratoire 1 – Sniffing

Ce laboratoire est noté - 11 points. 10% de la note finale

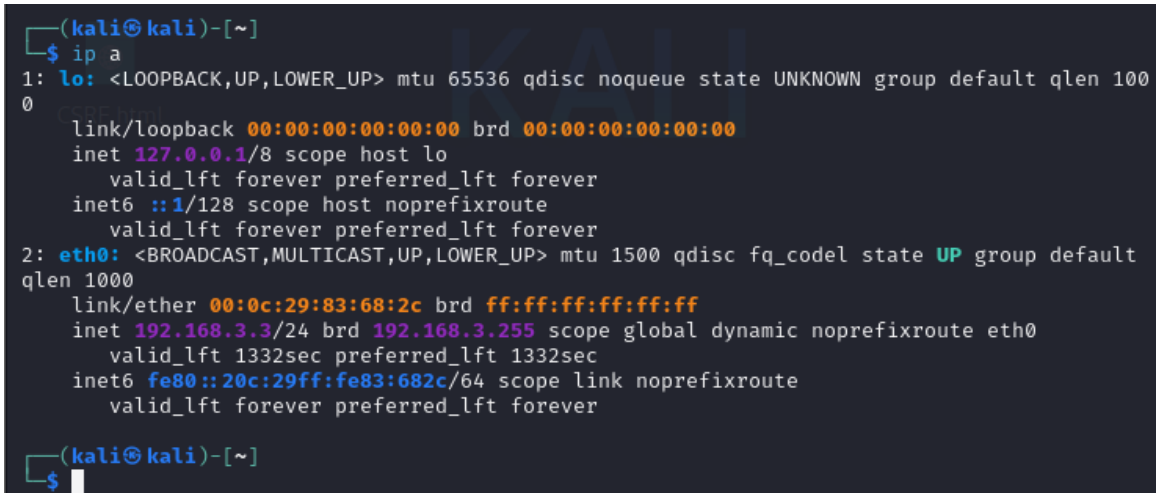
À rendre pour vendredi 17 janvier

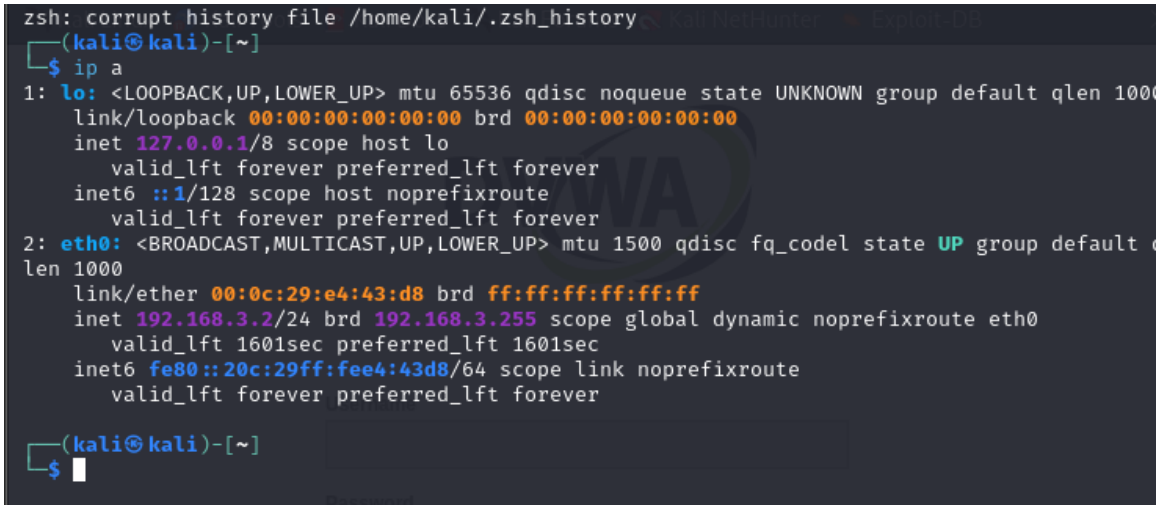
Au cours de ce laboratoire, vous serez un membre de la Purple Team. Vous devez mettreen place une attaque MitM ARP spoofing avec ettercap puis installer une contre-mesure efficace
contre cette attaque.

1 Mise en place du laboratoire (1 point)

Sous VirtualBox, installez 3 VMs Kali sur le même réseau interne : 1 VM Kali, 1 VM DVWA et

1 VM linux. Notez pour chacune leur adresse IP. (1 point)





```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 00:0c:29:7a:de:aa brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.3.4/24 metric 100 brd 192.168.3.255 scope global dynamic ens33
       valid_lft 1299sec preferred_lft 1299sec
    inet6 fe80::20c:29ff:fe7a:deaa/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

2 Tables ARP (1 point)

Vérifiez avec la commande ping que chaque VM peut communiquer avec les autres VMs. Puis,
notez la table ARP de chaque VM (donc 3 tables APR au total). (1 point)

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.2              ether   00:0c:29:e4:43:d8   C                     eth0
192.168.3.4              ether   00:0c:29:7a:de:aa   C                     eth0
192.168.3.1              ether   00:50:56:c0:00:02   C                     eth0
```

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.1              ether   00:50:56:c0:00:02   C                     eth0
192.168.3.3              ether   00:0c:29:83:68:2c   C                     eth0
192.168.3.254            ether   00:50:56:f5:0d:98   C                     eth0
192.168.3.4              ether   00:0c:29:7a:de:aa   C                     eth0

┌──(kali㉿kali)-[~]
```

```
ubuntu@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.1              ether   00:50:56:c0:00:02   C                     ens33
192.168.3.2              ether   00:0c:29:e4:43:d8   C                     ens33
192.168.3.3              ether   00:0c:29:83:68:2c   C                     ens33
192.168.3.254            ether   00:50:56:f5:0d:98   C                     ens33
ubuntu@ubuntu:~$
```

3 Sniffing ARP (3 points)
Sur la VM Kali que vous choisissez comme la VM d'attaque, utilisez l'outil ettercap pour mettre
en place une attaque ARP poisoning entre les 2 autres VMs. Montrez les tables ARP

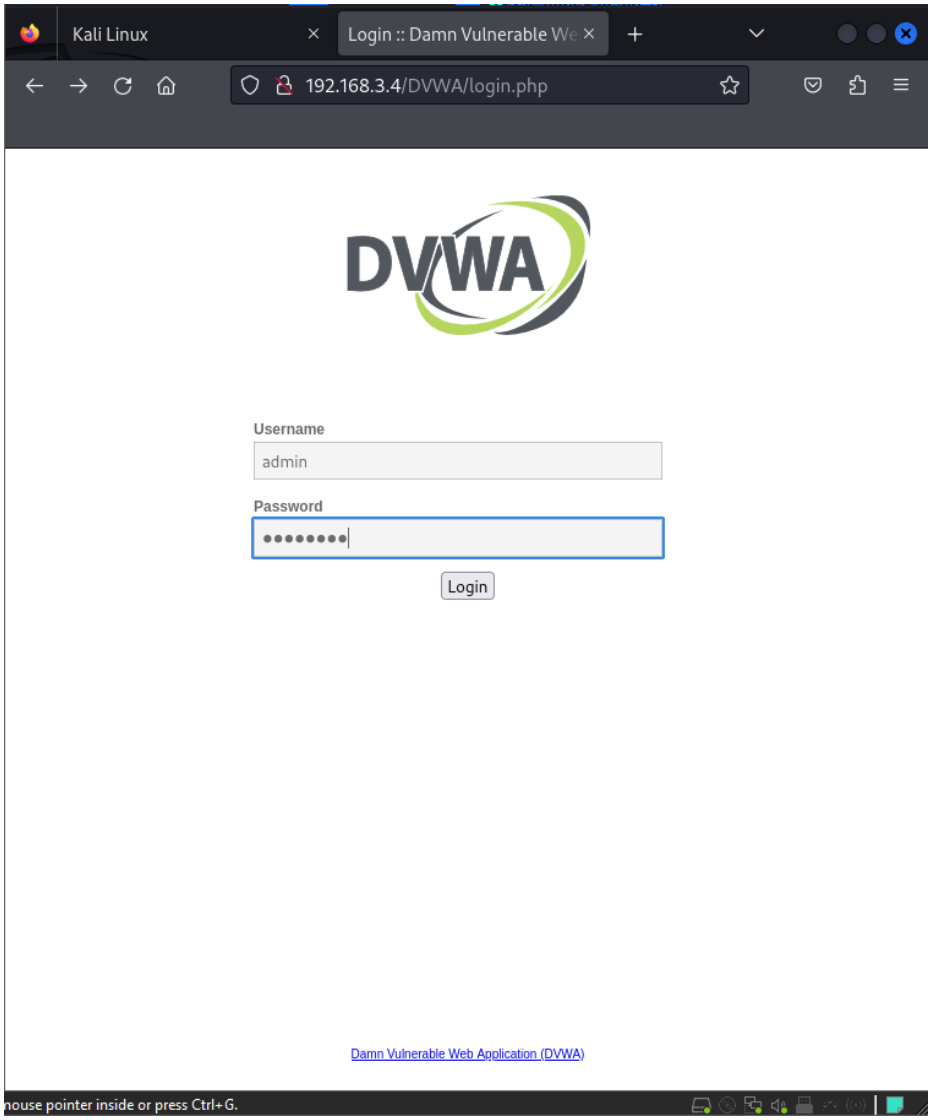
des deux
VMs cibles avant et après l'attaque. (2 points). Expliquez la différence. (1 point)

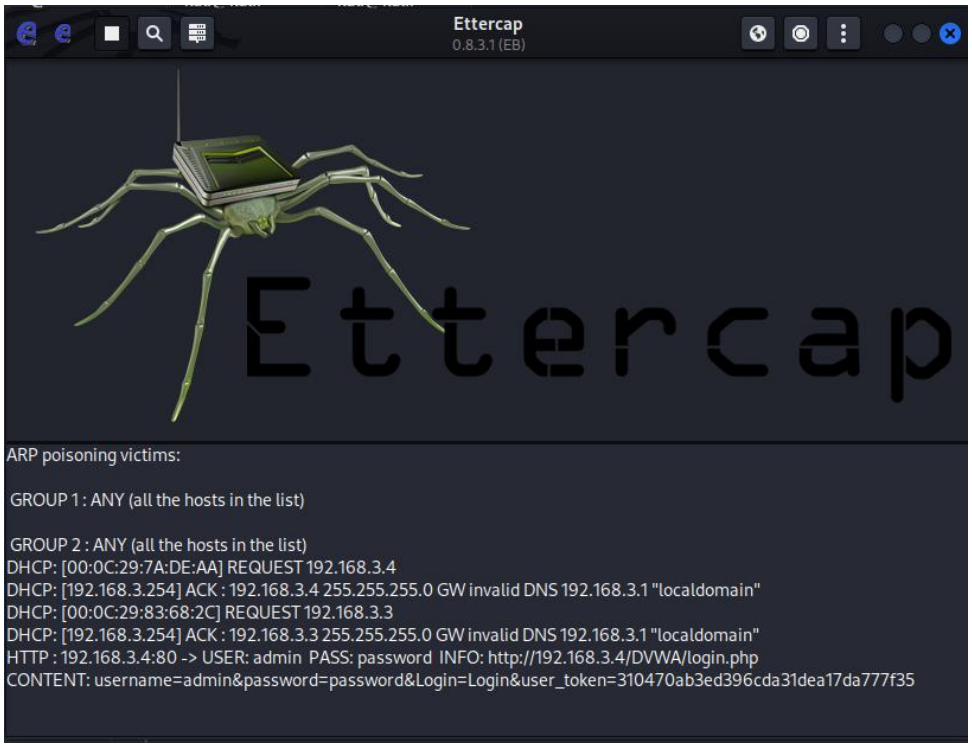
```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.254            ether   00:0c:29:e4:43:d8   C                     eth0
192.168.3.2              ether   00:0c:29:e4:43:d8   C                     eth0
192.168.3.4              ether   00:0c:29:e4:43:d8   C                     eth0
192.168.3.1              ether   00:0c:29:e4:43:d8   C                     eth0
```

```
ubuntu@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.1              ether   00:0c:29:e4:43:d8   C                     ens33
192.168.3.2              ether   00:0c:29:e4:43:d8   C                     ens33
192.168.3.3              ether   00:0c:29:e4:43:d8   C                     ens33
192.168.3.254            ether   00:0c:29:e4:43:d8   C                     ens33
ubuntu@ubuntu:~$
```

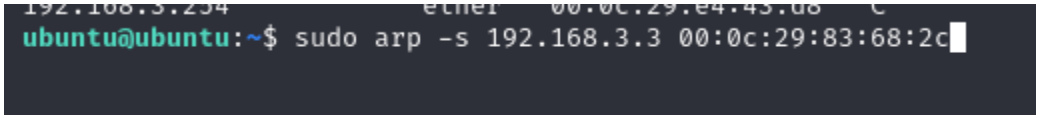
La différence entre les tables est qu'au numéro précédant chaque machine a sa propre adresse MAC et après l'attaque les machines ont l'adresse MAC de la machine qui attaque.

4 Attaque sniffing ARP (3 points)
Sur la VM Kali, utilisez l'outil ettercap pour écouter et capturer le mot de passe de connexion
de la VM Linux qui se connecte sur l'application DVWA. Montrez avec une capture écran que
l'identifiant et le mot de passe ont bien ét é capturés. (3 points)

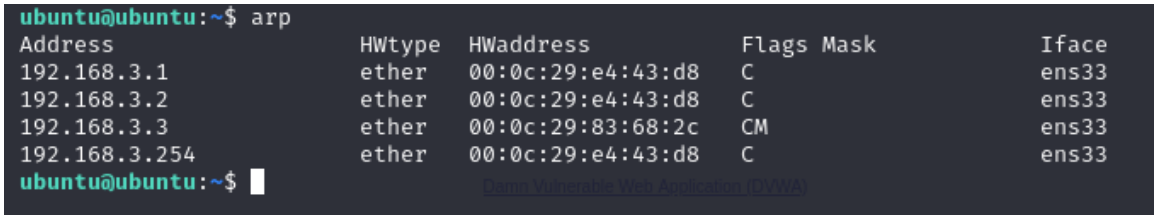

Kali Linux
Login :: Damn Vulnerable We
192.168.3.4/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
house pointer inside or press Ctrl+G.



5 Contre-mesure sniffing ARP (3 points)
Sur les VMs Linux et DVWA, mettez en place une contre-mesure efficace contre l'attaque ARP
poisoning. Expliquer la contre-mesure (1 point). Démontrez que la contre-mesure fonctionne contre ettercap à l'aide de captures écran. (2 points)



Mettre l'adresse en statique fait en sorte que lorsqu'on fait le ARP Poisonning l'adresse MAC ne change donc pas. L'attaque est donc bloquée.



Fin du laboratoire